EXHIBIT 1

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: **12/838,999**

Applicant: **LAMBERT, Robert John**

Filed: **July 19, 2010**

Title: **SYSTEM AND METHOD FOR REDUCING THE COMPUTATION AND STORAGE REQUIREMENTS FOR A MONTGOMERY-STYLE REDUCTION**

Art Unit: **2448**

Confirmation #: **7370**

Examiner: **TEAGUE, John e.**

Docket No.: **67539/01022**

Mail Stop Amendment
U.S. Patent & Trademark Office
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE

Sir:

This is further to the Office Action dated July 10, 2012. Applicant wishes to amend the above-identified application as follows:

Amendments to the Specification: begin on page 2 of this paper.

Amendments to the Claims: are reflected in the listing of claims which begins on page 4 of this paper.

Amendments to the Drawings: begin on page 8 of this paper and includes two attached replacement sheets.

Remarks: begin on page 9 of this paper.

Amendments to the Specification

Please replace paragraph [0030] of the application as filed with the following amended paragraph:

[0030] The cryptographic module 18 is configured to perform cryptographic operations such as encryption/decryption, signing and modular arithmetic, etc. In this example, the cryptographic module 18 is configured for performing elliptic curve cryptographic (ECC) operations, and includes a block Montgomery machine 22, further detail of which is shown in Figure 2. It will be appreciated that the cryptographic module 18 and any component thereof may be implemented as an apparatus in ~~either~~ hardware or in software (computer readable instructions embodied in/on a computer readable medium).

Please replace paragraph [0038] of the application as filed with the following replacement paragraph:

[0038] Turning now to Figure 4, an example is shown involving the reduction of a 10 word value a and a 5-word modulus n (i.e. $k=5$ iterations in this example where typically a is twice the length of n) comprising the words $a_9, a_8, a_7, a_6, a_5, a_4, a_3, a_2, a_1$, and a_0 according to the configuration shown in Figure 3, to illustrate the operations required in a typical Montgomery style reduction. In the first iteration, the multiplier m is computed using the least significant word a_0 and the value for μ stored locally in a register, and a value representative of m is stored for the next computation. Then $a+m\times n$ is computed using m and the initial representation of a. In the result, the least significant word a_0 is "zeroed" and a carry may be produced (shown in Figure [[3]] 4 after shifting). During this operation, or subsequently, the once operated upon values that remain, namely a_9', ..., a_2', and a_1', along with the carry c are fed into the next iteration, where the process is repeated. In the second iteration, the once operated upon value a_1', which is now the least significant word in the first intermediate representation of a is zeroed by computing m and then $a+m\times n$ is computed as before and the result shifted down one word. This is repeated for the remaining iterations resulting in a four times operated on carry c'''' and five times operated on values of the remaining words, since an

iteration for each word in n is applied. The four times operated on carry c'''' and the remaining values $a''_9, a''_8, a''_7, a''_6$, and a''_5 may then be used as an output representing $aR^{-1} \bmod n$.

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method for performing on a cryptographic apparatus a Montgomery-style reduction in a cryptographic operation, the method comprising:

obtaining a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction;

computing a modified operand by applying the modified reduction value, instead of the modulus, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof; and

outputting the modified operand.

2. (currently amended) The method according to claim 1 wherein the modified reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', w corresponds to a word size, and n corresponds to [[a]] the modulus.

3. (original) The method according to claim 1, wherein the computing further comprises:

successively applying the modified reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the operand; and

performing a standard Montgomery reduction on the most significant word of the operand.

4. (original) The method according to claim 3, wherein the performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value m, and overwriting the register with m.

5. (original) The method according to claim 1, wherein the cryptographic apparatus comprises a Montgomery engine configured to perform the cryptographic operation.

6. (original) The method according to claim 1, wherein the modified reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

7. (original) The method according to claim 1, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

8. (original) The method according to claim 7, wherein if a carry is produced during the computing, the outputting comprises adding the carry as a most significant word in the modified operand.

9. (original) The method according to claim 1, wherein said cryptographic operation comprises multiplication or squaring.

10. (currently amended) A cryptographic apparatus comprising a processor configured to operate as a Montgomery engine, and computer executable instructions that when executed by the processor ~~configured to~~:

obtain a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction;

compute a modified operand by applying the modified reduction value, instead of the modulus, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof; and

output the modified operand.

11. (currently amended) The apparatus according to claim 10, wherein said modified reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', w corresponds to a word size, and n corresponds to [[a]] the modulus.

12. (original) The apparatus according to claim 10, wherein the computing further comprises:

successively applying the modified reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the

operand; and

performing a standard Montgomery reduction on the most significant word of the operand.

13. (original) The apparatus according to claim 12, wherein performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value *m*, and overwriting the register with *m*.

14. (original) The apparatus according to claim 10, wherein the modified reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

15. (original) The apparatus according to claim 10, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

16. (original) The apparatus according to claim 15, wherein if a carry is produced during the computing, the apparatus is configured to add the carry as a most significant word in the modified operand.

17. (original) The apparatus according to claim 10, wherein the cryptographic operation comprises multiplication or squaring.

18. (currently amended) A non-transitory computer readable medium comprising computer executable instructions that when executed by a cryptographic apparatus, cause the cryptographic apparatus to:

obtain a modified reduction value, the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction;

compute a modified operand by applying the modified reduction value, instead of the modulus, to perform a replacement of a least significant word of the operand, rather than perform a cancellation thereof; and

output the modified operand.

19. (currently amended) The non-transitory computer readable medium according to claim 18, wherein said modified reduction value is $n' = 2^{-w} \bmod n$, or a shifted or signed version of n', *w* corresponds to a word size and *n* corresponds to [[a]] the modulus.

20. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the computing further comprises:

successively applying the modified reduction value to perform a replacement of each of the second least significant word of the operand through the second most significant word of the operand; and

performing a standard Montgomery reduction on the most significant word of the operand.

21. (currently amended) The non-transitory computer readable medium according to claim 20, wherein performing a standard Montgomery reduction comprises storing a precomputed value μ in a register, using the value μ in computing another value *m*, and overwriting the register with *m*.

22. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the modified reduction value is pre-computed and stored with one or more cryptographic system parameters prior to the computing.

23. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the performing comprises zeroing the least significant word of the operand, modifying one or more remaining words, and shifting one or more modified words, wherein the shifting is either logical or physical.

24. (currently amended) The non-transitory computer readable medium according to claim 23, wherein if a carry is produced during the computing, executing instructions to add the carry as a most significant word in the modified operand.

25. (currently amended) The non-transitory computer readable medium according to claim 18, wherein the cryptographic operation comprises multiplication or squaring.

Amendments to the Drawings

Please replace the drawing sheets containing Figure 3 and Figure 4 with the two replacement drawing sheets submitted herewith.

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Amendments to the Specification and Objections to the Specification

Paragraph [0030] of the description has been amended to clarify: "...may be implemented as an apparatus in hardware or in software".

Paragraph [0037] has been amended replacing "Figure 3" on line 9 with "Figure 4" as suggested by the Examiner.

Applicant respectfully submits that objections to the specification have been overcome.

Amendments to the Claims

Claim 1 has been amended to clarify: "the modified reduction value being a function of a modulus used in performing a standard Montgomery reduction" and that the modified reduction value is applied: "instead of the modulus". Support for these amendments can be found in at least Figures 6 and 7 (especially when compared to Figures 3 and 4) and paragraphs [0029] and [0041] through [0045] of the application as filed.

Claim 2 has been amended to be consistent with claim 1 as amended.

Claims 10 and 11 have been amended in a manner consistent with claims 1 and 2 as amended.

Claim 10 has also been amended to specify a "cryptographic apparatus comprising a processor configured to operate as a Montgomery engine, and computer executable instructions that when executed by the processor...". Support for these amendments can be found in at least paragraph [0030] and Figure 2 of the application as filed.

Claims 18 and 19 have been amended in a manner consistent with claims 1 and 2 as amended.

Claims 18-25 have been amended inserting "non-transitory" into the preamble of each claim as suggested by the Examiner.

Applicant respectfully submits that no new subject matter has been added by way of

these amendments.

Amendments to the Drawings and Drawing Objections

Figures 3 and 4 have been amended to specify that the drawings illustrate prior art. Applicant respectfully submits that Figures 3 and 4 thus amended overcome the Examiner's objections thereto.

Priority

Applicant notes that a foreign claim to priority has not been made, the ADS originally submitted included an incorrectly selected check box. Applicant hereby submits a corrected ADS.

Claim Rejections – 35 U.S.C. 101

Claims 10-17 have been rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter for allegedly claiming "software". Although Applicant does not necessarily agree with the Examiner, as detailed above, claim 10 has been amended to recite: "cryptographic apparatus comprising a processor configured to operate as a Montgomery engine, and computer executable instructions that when executed by the processor...". Applicant respectfully submits that claim 10 thus amended complies with 35 U.S.C. 101 and claims 11-17 being dependent thereon also comply with 35 U.S.C. 101

Claims 18-25 have been rejected under 35 U.S.C. 101 for being directed to non-statutory subject matter for reciting a "computer readable medium". As detailed above, "non-transitory" has been inserted into the preamble of each of claims 18-25 as suggested by the Examiner. Applicant respectfully submits that claims 18-25, thus amended, comply with 35 U.S.C. 101.

Claim Rejections – 35 U.S.C. 102 and 103

Claims 1, 3, 5-10, 12, 14-18, 20, and 22-25 have been rejected under 35 U.S.C. 102(b) as being anticipated by Sabin (EP 1,818,809). Claims 2, 11, and 19 have been rejected under

35 U.S.C. 103(a) as being unpatentable over Sabin in view of Romain (U.S. 6,424,987). Claims 4, 13, and 21 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sabin in view of Applicant Admitted Prior Art (AAPA). Applicant respectfully traverses the rejections as follows.

As outlined above, claim 1 has been amended to clarify that the modified reduction value is a function of a modulus and that it is used in computing a modified operand instead of the modulus.

Sabin may teach details of a Montgomery Reduction, however, Sabin does not teach or fairly suggest the use of a modified reduction value, let alone as recited in claim 1. For at least this reason, claim 1 is new with respect to Sabin.

The Applicant also respectfully submits that the claims are inventive over Sabin, Romain, and AAPA, for at least the following reasons.

As discussed in paragraphs [0028] to [0030] of the application as filed, to improve the reduction efficiency of a Montgomery machine, the objective should be to reduce the number of operations, especially word-by-word multiplication, and to maximize the number of components that can be kept in registers, reducing the loading and storing of temporary values.

In the present application, a system and method are utilized that provide an alternative way in which to produce a Montgomery reduction from below by storing a new precomputed value used to substantially replace the μ and n values used in a standard Montgomery reduction with a single value.

This may be done by storing a modified reduction value in the cryptographic apparatus, wherein the modified reduction value, when applied to an operand, input to or generated by, the cryptographic apparatus, performs a replacement for values in a low-order segment which is a target of the reduction, rather than a cancellation thereof, as performed in a standard Montgomery reduction; and performing the reduction from below using the modified reduction value.

By modifying the Montgomery reduction mechanism in this way, the number of multiplications and registers required to effect the Montgomery reduction can be reduced. To illustrate the effects of this modified Montgomery reduction, an example of a cryptographic system and Montgomery architecture within such a system will first be described.

Sabin does not recognize the above-noted efficiencies, let alone how they can be attained. It is respectfully submitted that claim 1 as amended is clearly and patentably distinguished over Sabin.

With respect to Romain, Applicant respectfully submits that the Examiner is reading too much into the teachings relied upon. Particularly, Applicant notes that the expression $I = 2^{-n} \bmod N$ on line 37 of column 1 is not equivalent to the modified reduction value described in the present application. First, in Romain, I is a binary data element called an error. There is nothing in Romain that suggests the form of the error could be applied to a modified reduction value. In fact, Romain does not teach or suggest a modified reduction value. Second, $I = 2^{-n} \bmod N$ does not incorporate the word size, as is recited in claim 2 (i.e. *w*), the number of bits *n* is used. Finally, $I = 2^{-n} \bmod N$ appears to be reduced by a binary data element N. Romain does not suggest that the value N is the modulus.

For at least these reasons, Applicant respectfully submits that claims 1-25 are patentable over Sabin in view of Romain.

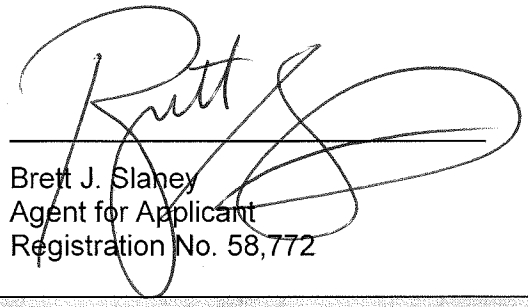
With respect to AAPA, although Figure 3 of the present application illustrates a standard Montgomery reduction, there is nothing in the present application that suggests performing a standard Montgomery reduction on the most significant word of the operand after applying the modified reduction value as recited in claim 3, is part of the prior art.

For at least the above reasons, Applicant respectfully submits that claims 1-25 are both novel and patentable over the cited references.

* * *

In view of the foregoing, Applicant respectfully submits that the present application is in condition for allowance and therefore requests early reconsideration and allowance of the present application.

Respectfully submitted,



Brett J. Slaney
Agent for Applicant
Registration No. 58,772

Date: October 10, 2012

Blake, Cassels & Graydon LLP

199 Bay Street
Suite 4000, Commerce Court West
Toronto ON M5L 1A9
Canada

Tel: 416-863-2518

BS/sdb